All FSA System Findings

Total of All System Findings: 363

(Open, Closed, and Unknown)

System Name	*Finding*	*Status*	*Concur/ Nonconcur*	*Date Reported*	*Date Closed*	*Sources*
CDDTS 2	The configuration management plan does not demonstrate that system software has been properly licensed	Unknown		11/10/2003		C&A
CDDTS 3	Audit trails are not retained for 1 year as required by policy	Unknown		11/10/2003		C&A
CDDTS 4	Passwords are not changed in 90 days as required by policy	Unknown		11/10/2003		C&A
CDDTS 5	No documented procedures describing creation of emergency passwords	Unknown		11/10/2003		C&A

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
CDDTS 6	No documented procedures describing limitation regarding access scripts with embedded passwords	Unknown		11/10/2003		C&A
CDDTS 7	The configuration management plan should include the following hardware information: vendor name, serial and model numbers	Unknown		11/10/2003		C&A
CDDTS 1	The configuration management plan does not contain current version of system software	Unknown		11/10/2003		C&A Precert
COD 9	There is not an efficient and consistent process to ensure users are promptly removed from the system	Unknown	Unknown			
COD 3	The dept. has systems without or that need updated SSPs that identify the vulnerabilities and potential threates to systems and the controls in place to secure information systems	Open	Unknown			2001 annual program review GAO-01-1067 IG GISRA

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
COD 2	The dept. has not fully implemented a risk-based, comprehensive agencywide security program that ensures the adequate application of security controls	Closed	Unknown			2002 POAM
COD 1	Finalize security training	Closed	Concur			2002 risk assessment
COD 4	Need to review contingency plans	Closed	Unknown			2002 risk assessment
COD 6	An excessive number of users have accounts on the system	Unknown	Unknown	11/1/2003		IGIC-03
COD 7	There are an excessive number of user accounts assigned to administrator security groups	Unknown	Unknown	11/1/2003		IGIC-03

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
COD 8	There are no adequate controls in place to limit an individual's access to the COD system. Controls around granting user access to the COD system are not operating effectively	Unknown	Unknown	11/1/2003		IGIC-03
COD 10	There is no formal procedure or requirement in place for COD to periodically monitor user accounts for improper access privileges	Unknown	Unknown	11/1/2003		IGIC-03
COD 11	The system security plan does not explain the specific responsibilities and expectations of the system security officers	Unknown	Unknown	11/1/2003		IGIC-03
COD 12	The disaster recovery plan does not address critical data files	Unknown	Unknown	11/1/2003		IGIC-03
COD 13	The disaster recovery plan does not address procuedure to be followed when the data service center cannot receive or transmit data	Unknown	Unknown	11/1/2003		IGIC-03

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
COD 14	The disaster recovery plan does not address procedures for regeneration of the system files	Unknown	Unknown	11/1/2003		IGIC-03
COD 15	The disaster recovery plan does not address how the plan will be distributed to the appropriate personnel	Unknown	Unknown	11/1/2003		IGIC-03
COD 16	Program change controls: The release document, which serves as a summarized planning document with explanations of the proposed changes, did not contain any information related to the change selected for testing	Unknown	Unknown	11/1/2003		IGIC-03
CPS 3	Background checks are not performed on date entry personnel at the MDE facility	Unknown	Unknown			2002 risk assessment
CPS 4	Sensitive information is stored securely either in the facility itself or in a bonded storage facility. However, backup media are written over rather than erased. Moreover, at Mt. Vernon, corrupted RAID drives must be returned to the	Unknown	Unknown			2002 risk assessment

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
CPS 1	Training elements don't include incident reporting for all personnel.	Unknown	Unknown	12/2/2003		C&A
CPS 2	The department has no MOUs with connected sytems	Unknown	Unknown			EDS vulnerability assessment
DCSS 1	The FFEL system user accounts are not automatically disabled after 90 days of inactivity	Closed	Unknown			2002 risk assessment
DCSS 2	The FFEL system SSP does not reflect the current configuration of the system and needs to be updated.	Closed	Concur			2002 risk assessment
DCSS 3	New employees are not required to formally acknowledge their understanding of the security awareness guidelines	Unknown	Unknown	11/1/2003		IGIC-03

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DCSS 4	There are no formal procedures for conducting periodic reviews of user access privileges to the DCSS application for contractor employees.	Unknown	Unknown	11/1/2003		IGIC-03
DCSS 5	Remote access is not formally revalidated on a periodic basis.	Unknown	Unknown	11/1/2003		IGIC-03
DLCS 2	The dept. has not fully implemented a risk-based, comprehensive agencywide security program that ensures the adequate applicatin of security controls	Closed	Unknown			2002 POAM
DLCS 1	Unlimited concurrent logins are allowed	Open	Unknown			2002 risk assessment
DLOS 1	Windows NT and UNIX security audits are not fully documented	Open	Concur			2002 risk assessment

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLOS 2	Computer security incidents continue to be tracked and recorded manually	Open	Unknown			2002 risk assessment
DLSS 88	There was no evidence documenting whether or not public access was allowed to DLSS.	Open	Unknown			2002 risk assessment
DLSS 89	Choke Cherry LAN system resources are not controlled to ensure constant and consistent availability.	Closed	Unknown			2002 risk assessment
DLSS 90	Access to Choke Cherry LAN server room using an existing control system is unregulated	Closed	Concur			2002 risk assessment
DLSS 91	Development protocols for Web applications are inconsistent with project standards	Closed	Concur			2002 risk assessment

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 92	Statistical analysis to spot abnormal activity patterns that may indicate an attack is not performed proactively. Applies to T1, Utica T1, and Bakersfield T2	Open	Concur			2002 risk assessment
DLSS 93	Choke Cherry LAN users are not required to change passwords on a periodic basis.	Closed	Concur			2002 risk assessment
DLSS 94	ED regulation requires training when an employee enters a new position that deals with sensitive information. This guidance is not followed at the Center. (applies to utica M2, bakersfield m2, dallas m2, southgate m2-completed for ALL	Closed	Nonconcur			2002 risk assessment
DLSS 95	The classification of sensitive data that requires protection shall be determined. Appropriate action will be taken to ensure that proper labeling banners are attached to documents.	Closed	Concur			2002 risk assessment
DLSS 96	Vulnerability scanners used to identify weaknesses that could lead to security violations and uncover possible breaches are used in a reactive mode. (bakersfield m4)	Closed	Concur			2002 risk assessment

All FSA Findings—Open, Closed, and Unknown

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 97	Technical controls to ensure appropriate security controls are specified, designed into and accepted in the application in accordance with NIST guidance are not completed. NOTE: completed for utica t3, bakersfield t4; ongoing for dallas t1, southgate t1	Open	Concur			2002 risk assessment
DLSS 98	LAN user IDs are permitted to initiate multiple concurrent logins to the LAN network note: applies to utica t4, bakersfield t5, dallas t2, southgate t2--completed for all these	Closed	Concur			2002 risk assessment
DLSS 99	Terminals, workstations and networked personal computers are left unattended when user ID and password have been logged-in. Note: applies to utica t5, bakersfield t6, dallas t3, southgate t3 and t4, irs t1--completed for all	Closed	Concur			2002 risk assessment
DLSS 100	UPS is not tested on a quarterly basis. Note: applies to dallas 01, bakersfield 01	Closed	Concur			2002 risk assessment

All FSA Findings—Open, Closed, and Unknown

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 101	The integrity of all data files is not assessed. This is specific to production user files and LAN operating system files. NOTE: applies to bakersfield t1	Closed	Concur			2002 risk assessment
DLSS 102	Security cameras and or guards are utilized to protect the building from unauthorized access and to record security violations. However, we found one area that remains vulnerable because of lack of monitoring. Note: applies to dallas 02, southgate 01, ABR 01--completed for all	Closed	Concur			2002 risk assessment
DLSS 103	Escorts are not for unauthorized individuals at all times. Note: applies to southgate 02	Closed	Concur			2002 risk assessment
DLSS 104	Procedures to ensure that compliance with the Privacy Act is not consistently observed. Note: applies to electronic debit m1, DCS m1--completed for all	Closed	Concur			2002 risk assessment

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 105	Segregation of duties within the IT function should be strengthened. Note: applies to SAIG m1	Closed	Concur			2002 risk assessment
DLSS 106	There is no timely validation of data received. Note: applies to FMS t1	Closed	Concur			2002 risk assessment
DLSS 107	Standards should have minimum expected control guidance including: operations controls, input/output handling controls, and technical support. Note: applies to SAIG M2	Closed	Concur			2002 risk assessment
DLSS 86	No means of tracking user compliance of annual security awareness training	Unknown	Unknown	11/13/2003		C&A
DLSS 87	Rules of behavior have not been established to delineate the responsibilities and expected behavior of all individuals with access to the application. The rules should state the consequences of inconsistent behavior.	Unknown	Closed	11/13/2003	1/19/2004	C&A

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 1	Identified several servers containing administrator accounts with blank or simple passwords; gained unauthorized access with administrator rights.IG Action Memo: Fourteen Servers contain administrator accounts with identical user accounts names and passwords or no defined password…IG Action Memo: Three NT Servers allow anonymous access to the Windows NT system registry…	Closed	Concur		4/25/2003	IG
DLSS 2	Database servers contain accounts with same username and passwordIG Action Memo: Four Databases contain accounts with default usernames and passwords or accounts with identical username and passwords…	Closed	Concur		4/25/2003	IG
DLSS 3	Identified server containing “Unicode” vulnerability allowing us to gain unauthorized access to the server’s operating systemIG Action Memo: An Intranet web server contains an Unicode vulnerability that allows an attacker to gain unauthorized access to the servers’ operating system files and	Closed	Concur		5/8/2003	IG
DLSS 4	Identified servers providing anonymous FTP services which allowed upload of any fileIG Action Memo: Six servers provide File Transfer Protocol (FTP) services that contain commonly known security vulnerabilities…	Closed	Concur		5/8/2003	IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 5	Identified Compaq Insight Manager sessions that allow logon using the “operator” username and password.IG Action Memo: Most Windows NT servers utilize an outdated version of Compaq Web Management Server (CWMS)...	Closed	Concur		5/25/2003	IG
DLSS 6	Identified several servers providing SNMP service with the default passwords.IG Action Memo: Fifteen servers utilize Simple Network Management Protocol (SNMP) services with the default passwords…	Closed	Concur		5/25/2003	IG
DLSS 7	Identified several NT servers that allow anonymous connections via the “netbios null session.”IG Action Memo: Most Windows NT servers that we tested had Netbios registry settings configured to all Anonymous (null) connections to its default shares (i.e., IPC$)…	Closed	Concur		5/25/2003	IG
DLSS 8	IDS is not installed on network segments; external vulnerability scans were not detected by an alert mechanismIG Action Memo: We noted that a network based IDS systems did not detect our intrusive vulnerability scanning…	Closed	Concur		5/15/2003	IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 9	Norton Anti-virus is not installed on NT ServersIG Action Memo: We determined that sufficient controls have not been implemented to protect Internet facing servers from contracting common computer viruses…	Closed	Concur		5/31/2003	IG
DLSS 10	Database servers containing sensitive data should not reside within the DMZIG Action Memo: We conducted procedures to determine whether logical access controls have been implemented to protect critical DLSS data residing on data base servers...	Closed	Concur		5/18/2003	IG
DLSS 11	DLSS is not logically segregated from the ACS corporate networkIG Action Memo: We determined whether logical access controls have been implemented to segregate DLSS from potentially un-trusted networks at the RCC…	Closed	Concur		6/13/2003	IG
DLSS 12	Tripwire is not installed on servers within the DMZ environment	Closed	Concur		5/31/2003	IG
DLSS 13	Database server contained an “sa” account with no password defined	Closed	Concur		4/25/2003	IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 14	Auditing is not enabled	Closed	Concur		5/18/2003	IG
DLSS 15	Latest service pack not installed on SQL Server 7.0	Closed	Concur		4/25/2003	IG
DLSS 16	Evidence of periodic review of server audit logs, and firewall logs is not documented	Closed	Concur		5/30/2003	IG
DLSS 17	System Security Plan does not address roles and responsibilities of system administrators	Closed	Concur		5/2/2003	IG
DLSS 18	System administrator duties, authorization levels, and scope of responsibilities are not documented	Closed	Concur		5/2/2003	IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 19	Documented baseline security requirements for servers and network devices have not been developed	Closed	Concur		5/30/2003	IG
DLSS 20	Security Guard at Rockville Data Center is not required to check bags for unusual items	Closed	Nonconcur			IG
DLSS 21	Security Camera positions do not allow guard to view areas next to the building	Closed	Concur		5/27/2003	IG
DLSS 22	Complete reconciliation of data tapes contained at ACS and Iron Mountain is not performed	Closed	Nonconcur			IG
DLSS 23	Employee files did not contain documentation indicating that ACS contractors have met the Department's IT security training requirements (Security Awareness Training)	Closed	Concur		6/2/2003	IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 24	Not all ACS employee files contained system authorization forms granting access to Department systems	Closed	Concur		5/8/2003	IG
DLSS 25	Certain ACS employees have not submitted the required paperwork for background investigations	Closed	Concur		5/22/2003	IG
DLSS 26	Identified many accounts that contain passwords that do not expire.	Closed	Concur		5/22/2003	IG
DLSS 27	Oracle database contains several default user accounts and passwords.	Closed	Concur		4/25/2003	IG
DLSS 28	External vulnerability scans identified a DNS server that is not using the most recent version of the DNS application	Closed	Concur		5/8/2003	IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 29	Identified servers that utilize “rhosts and rlogin” services; trust relationships.	Closed	Concur		4/25/2003	IG
DLSS 30	Open SSH has not been implemented on servers that utilize FTP and Telnet	Closed	Concur		5/8/2003	IG
DLSS 31	Certain FTP servers do not contain warning banners about Government facility	Closed	Concur		5/15/2003	IG
DLSS 32	Identified servers running PC Anywhere requiring no password authentication	Closed	Concur		4/25/2003	IG
DLSS 33	Identified a server using a version of “Sendmail” that may be vulnerable to a SMTP Pipe attack	Closed	Concur		4/25/2003	IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 34	Open VMS contained a vulnerability identified by Akita Security (UK)	Closed	Concur		4/11/2003	IG
DLSS 35	Purchase of the full version of Stoat Security Scanner for OpenVMS may be helpful for identifying other security weaknesses.	Closed	Concur		5/28/2003	IG
DLSS 36	Rockville administrators are not using a variety of vulnerability scanning tools to identify and correct common security vulnerabilities and exposures	Closed	Concur		5/30/2003	IG
DLSS 37	Complex password policy is not being enforced on system administrator and user accounts. Suggest running password cracker to identify weak passwords.	Closed	Concur		5/30/2003	IG
DLSS 38	User Account Lockout Feature Is Not EnabledIG Action Memo: noted that the administrators have not enabled the user account lockout feature to limit the number of failed login attempts to databases containing sensitive data...	Unknown	Concur		12/15/2003	IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 39	Database Link Password Encryption/Login Encryption Parameter Settings are not Secure IG Action Memo noted that the "DBLINK_ENCRYPT_LOGIN" or the "ORA_ENCRYPT_LOGIN" parameter settings is not configured to encrypt stored passwords or encrypt users passwords when users connect to the database…	Unknown	Concur		12/15/2003	IG
DLSS 40	User Account Granted the CONNECT Default RoleIG Action Memo: noted that numerous user accounts are granted the CONNECT Default Role for database connections…	Unknown	Concur		12/15/2003	IG
DLSS 41	User Accounts Assigned to the Default System TablespaceIG Action Memo: noted that certain user accounts are assigned the default tablespace of SYSTEM…	Unknown	Concur		12/15/2003	IG
DLSS 42	Guest User Accounts Are Not DisabledIG Action Memo: noted that guest user accounts have not been disabled …	Unknown	Concur		12/15/2003	IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 43	User Accounts Can Execute CmdExec and Active Scripting JobsIG Action Memo: identified four SQL Server databases (RCC = 2) that allowed any user to execute CmdExec and Active Scripting jobs...	Unknown	Concur		12/15/2003	IG
DLSS 44	Statement Permissions Granted to User AccountsIG Action Memo: identified four SQL Server databases (RCC = 1) that had granted “STATEMENT” permissions to various user accounts…	Unknown	Concur		12/15/2003	IG
DLSS 45	Excessive Permissions Granted to the Public GroupIG Action Memo: noted that the “PUBLIC” group had been granted excessive permissions to include delete, insert, references, select, and update rights of database objects…	Unknown	Concur		12/15/2003	IG
DLSS 46	System Table Permissions Granted to the Public GroupIG Action Memo: On one SQL Server database at the RCC, noted that the “PUBLIC” sensitive information, such as login IDs, permissions, and database objects, access to these tables should be restricted from the “Public” group…	Unknown	Concur		12/15/2003	IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 47	Account LockoutIG Action Memo: noted that all 10 servers tested at the RCC have not configured settings to lock out accounts after a specified number of unsuccessful logon attempts…	Unknown	Concur		12/15/2003	IG
DLSS 48	Default Administrator Accounts & Console RestrictionIG Action Memo: discovered that the default administrator account was not renamed on three servers at the RCC and that the administrator account was not restricted to the console interface on all 10 servers tested…	Unknown	Concur		12/15/2003	IG
DLSS 49	Disabling LANMAN Authentication on Domain ControllersIG Action Memo: noted that domain controllers at the RCC were not configured to disable LANMAN user authentication over the network…	Unknown	Concur		12/15/2003	IG
DLSS 50	Change System TimeIG Action Memo: noted that on most servers tested (RCC = 7), the Power Users, Administrators, and Server Operators had permission to perform this function…	Unknown	Concur		12/15/2003	IG
DLSS 51	Shut Down SystemIG Action Memo: noted that on all servers tested at the RCC, the Power Users, Administrators, Server Operators, and Backup Operators had permission to perform this function…	Unknown	Concur		12/15/2003	IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 52	Act as Part of Operating SystemIG Action Memo: noted that on many servers tested (RCC = 3), the Administrators or Everyone user group had permission to perform this function…	Unknown	Concur		12/15/2003	IG
DLSS 53	Bypass Traverse CheckingIG Action Memo: noted that on all servers tested at the RCC, the Everyone user group had permission to perform this function…	Unknown	Concur		12/15/2003	IG
DLSS 54	Permissions on Memory Dump FilesIG Action Memo: noted that on one server at the RCC, the Everyone user group had full access to the memory dump file...	Unknown	Concur		12/15/2003	IG
DLSS 55	Excessive Permissions on System Files and DirectoriesIG Action Memo: noted that on most servers tested at the RCC and EDNet, the Everyone user group had full access to the following critical system files and directories…	Unknown	Concur		12/15/2003	IG

All FSA Findings—Open, Closed, and Unknown

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 56	World Writable FilesIG Action Memo: noted that a number of servers (RCC = 2) contained files that were assigned permissions allowing any user to access certain files and directories, modify their contents, and execute various functions. We also identified world writeable configuration files in the /etc directory that provide for any process to have the ability to alter the configuration of the system seizing unauthorized resources or denying resources to authorized users…	Unknown	Concur		12/15/2003	IG
DLSS 57	Excessive Set-User ID/Set-Group ID (SUID/SGID) FilesIG Action Memo: identified 5 servers at the RCC that contained excessive files with imbedded SUID and SGID permissions…	Unknown	Concur		12/15/2003	IG
DLSS 58	Use of hosts.equiv and rhosts files IG Action Memo: identified several servers (RCC = 3) containing hosts.equiv and rhosts files which indicates that trust relationships have been established with other systems on the network. In addition, we noted that these files contain a root user account, …	Unknown	Concur		12/15/2003	IG
DLSS 59	Firmware Security Mode and Password are not UtilizedIG Action Memo: identified two Sun Solaris servers at the RCC that have not enabled the firmware security mode and password (EEPROM) setting…	Unknown	Concur		12/15/2003	IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 60	System Files and Directories not Owned by RootIG Action Memo: identified three servers at the RCC that contain key system files and directories (e.g., /etc, /dev, /bin, and /usr/etc) that are not owned by root…	Unknown	Concur		12/15/2003	IG
DLSS 61	Unique Universal Identification Code (UIC) for all User AccountsIG Action Memo: noted that the majority of online user accounts were assigned the same UIC, which results in a loss of individual accountability within DLSS…	Unknown	Concur		12/15/2003	IG
DLSS 62	Authorization and Access Control List (ACL) Event Classes are not Enabled IG Action Memo: noted that the Authorization and ACL event classes are not enabled to capture security related …	Unknown	Concur		12/15/2003	IG
DLSS 63	EnableForcedLogoffIG Action Memo: discovered that most servers (RCC = 2 and VDC = 10) had not configured this setting to allow Administrators to force users to log off when needed...	Unknown	Concur		12/15/2003	IG
DLSS 64	AutodisconnectIG Action Memo: discovered that most servers (RCC = 2 and VDC = 7) had not configured this setting to allow Administrators to disconnect users if needed...	Unknown	Unknown		12/15/2003	IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 65	IOS – Defining a Telnet Access Control List (ACL)IG Action Memo: noted that the routers at the RCC have not adequately defined an ACL to limit the number of Telnet (Virtual Type Terminal (VTY) ports) connections and corresponding IP addresses that are able to log onto the router..	Unknown	Concur		12/15/2003	IG
DLSS 66	IOS – Exec TimeoutIG Action Memo: noted that routers at RCC have not defined IOS – Exec Timeout parameter on all console and auxiliary interfaces...	Unknown	Concur		12/15/2003	IG
DLSS 67	IOS – TCP Keepalive ServiceIG Action Memo: noted that the routers at the RCC have not enabled this service to terminate connections if the host on the other end of an idle connection has been lost…	Unknown	Concur		12/15/2003	IG
DLSS 68	IOS – No IP Source RouteIG Action Memo: noted that two routers at the RCC have not defined the IOS – No IP Source Route parameter to mitigate against well known Denial of Service attacks associated with the service...	Unknown	Concur		12/15/2003	IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 69	IOS – No IP Proxy Address Resolution Protocol (ARP)IG Action Memo: noted that the routers at the RCC have not implemented this parameter to mitigate against trust relationships created by this service…	Unknown	Concur		12/15/2003	IG
DLSS 70	IOS – Network Time Protocol (NTP) Server/SourceIG Action Memo: noted that the routers at the RCC have not defined the IOS – NTP Server/Source parameter that is required for communication and time synchronization with other NTP servers…	Unknown	Concur		12/15/2003	IG
DLSS 71	IOS – VTY Transport TelnetIG Action Memo: noted that the routers at the RCC have not defined this parameter to ensure that only telnet connections are allowed for remotely accessing routers and will ensure that other unsecured protocols (e.g. rlogin, WWW) can	Unknown	Concur		12/15/2003	IG
DLSS 72	IOS – Logging Trap InfoIG Action Memo: noted that most routers at the RCC have not defined this parameter to allow administrators to configure the severity level of messages that will generate SNMP trap messages...	Unknown	Concur		12/15/2003	IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 73	IOS – No IP Bootp Server IG Action Memo: noted that most routers at the RCC have not defined this parameter to disable the Bootp service in accordance with vendor recommended settings...	Unknown	Concur		12/15/2003	IG
DLSS 74	IOS – Service StampsIG Action Memo: noted that the routers at the RCC had not enabled this service to ensure that logging messages are timestamped...	Unknown	Concur		12/15/2003	IG
DLSS 75	Insufficient Disk CapacityIG Action Memo: noted that a number of servers (RCC = 1,) were experiencing disk utilization rates greater than 90 percent and therefore may not have sufficient disk capacity to perform normal	Unknown	Concur		12/15/2003	IG
DLSS 76	Allocate FloppiesIG Action Memo: noted that on the majority of servers tested (RCC = 7,), this setting was not configured to restrict use of the floppy drive to users logged onto the console interface…	Unknown	Concur		12/15/2003	IG
DLSS 77	Allocate CDROMSIG Action Memo: noted that on the majority of servers tested (RCC = 7,), this setting was not configured to restrict use of the CDROM drive to users logged onto the console interface…	Unknown	Concur		12/15/2003	IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 78	AutoAdminLogonIG Action Memo: discovered that on most servers tested (RCC = 6), this setting was not configured to prevent unauthorized users from bypassing Windows NT authentication processes and gaining administrator privileges…	Unknown	Concur		12/15/2003	IG
DLSS 79	DontDisplayLastUsersNameNote: this same vulnerability is listed twice in report.IG Action Memo: noted that on most servers tested (RCC = 10,), this setting was not configured to prevent displaying the last user's account name during subsequent logon sessions...	Unknown	Concur		12/15/2003	IG
DLSS 80	CGI File and Scripting Content Disclosure Vulnerability IG Action Memo: certain servers (RCC = 4) contain CGI files and scripts (e.g., htiimage.exe, search.vts, /WEB-INF/ directory, viewersrc.cgi) that allow an attacker to view certain system files and directories on the remote servers and may allow attacker to execute arbitrary	Unknown	Concur		12/15/2003	IG
DLSS 81	LanMan (LM) Hash System Vulnerability IG Action Memo: identified seven servers at the RCC that have enabled the LM hash setting for user authentication. LM uses a weak encryption scheme and passwords can be broken in a very short period of time, allowing an attacker to gain access to the system. …	Unknown	Concur		12/15/2003	IG

All FSA Findings—Open, Closed, and Unknown

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 82	IIS Sample Application FilesIG Action Memo: identified one server at the RCC that contained sample application files that are provided during default installation of Microsoft IIS …	Unknown	Concur		12/15/2003	IG
DLSS 83	Web Server MSADC Showcode VulnerabilityIG Action Memo: identified one server at the RCC that contains the “showcode.asp” file, which allows anyone with a web browser to view the contents of any text file on the web server, including files that are outside of the document root of the web server…	Unknown	Concur		12/15/2003	IG
DLSS 84	Audit Logging does not utilize Audit and Alarm Access Control Entries (ACE)IG Action Memo: noted that the audit function within DLSS is not configured to utilize Audit and Alarm ACE’s to track user activity and identify unauthorized attempts to modify log files…	Unknown	Concur		12/15/2003	IG
DLSS 85	System Parameters do not comply with Vendor Recommended SettingsIG Action Memo: noted that the DLSS security system parameter “RMS_FILEPROT” is configured with the default file protection setting (64,000.. also noted that the “SECURITY POLICY” parameter (7) is configured to not notify security operator terminals in the event that a system intrusion has been identified…	Unknown	Concur		12/15/2003	IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 108	Access request forms are not signed off by the appropriate manager	Unknown	Unknown	11/1/2003		IGIC-03
DLSS 109	Access request forms not complete or having pages missing	Unknown	Unknown	11/1/2003		IGIC-03
DLSS 110	Actual access rights differ from the access rights listed on the request forms	Unknown	Unknown	11/1/2003		IGIC-03
DLSS 111	47 percent of the separated employees tested did not have their eCRM account removed, and that 27 percent of the separated employees did not have their green screen account removed	Unknown	Unknown	11/1/2003		IGIC-03
DLSS 112	Access-rights reviews do not include an evaluation of curent user's access rights to the system.	Unknown	Unknown	11/1/2003		IGIC-03

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
DLSS 113	Audit trails: No functionality in place to track the activities performed by system administrators	Unknown	Unknown	11/1/2003		IGIC-03
DLSS 114	There is no documented policy or procedure that serves as a guideline for the process of identifying, evaluating, and implementing security patches for the infrastructure that supports DLSS.	Unknown	Unknown	11/1/2003		IGIC-03
DLSS 115	There is no formal tracking mechanism for security incidents, their status, and their resolution	Unknown	Unknown	11/1/2003		IGIC-03
DLSS 116	The DLSS security plan does not contain documented procedures that define the monitoring process for DLSS' compliance with FSA's security regulations and guidelines.	Unknown	Unknown	11/1/2003		IGIC-03
DLSS 117	There is a lack of appropriate segregation of duties over the change management process for DLSS.	Unknown	Unknown	11/1/2003		IGIC-03

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 90	Receive official system certification and accreditation	Open	Unknown			2001 annual program review GAO-01-1067 IG IG GISRA
ECB 85	Develop/update NIST-compliant system security plan NOTE: Finding also	Open	Concur			2001 annual program review IG GAO-01-1067
ECB 77	The department has systems withought or that need updated system security plans that identify the vulnerabilities and potential threats to systems and the contrtols in place to secure information systems	Closed	Concur			2002 POAM
ECB 78	The department has systems withought or that need updated system security plans that identify the vulnerabilities and potential threats to systems and the contrtols in place to secure information systems (CAP: Complete operational controls section of SSP)	Closed	Concur			2002 POAM

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 81	Complete the Operational Controls section of the SSP	Closed	Concur			2002 POAM
ECB 83	Establish and document a configuration management process	Open	Concur			2002 POAM
ECB 86	Complete technical controls section of SSP	Closed	Concur			2002 POAM
ECB 88	Complete a security testing and evaluation plan.	Open	Concur			2002 POAM
ECB 89	Submit all certification and accreditation documentation to the Certification Review Group (CRG).	Open	Unknown			2002 POAM

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 75	Ensure compliance with all federal and departmental policies and guidelines explicitly noted in the ECB system security plan	Closed	Concur			2002 risk assessment
ECB 76	Incorporate SFA's security life cycle checklists into the continuous development of ECB	Open	Unknown			2002 risk assessment
ECB 79	Increase the granularity of the ECB input/output documentation. This area should have detailed controls addressing specific input/output security measures.	Open	Unknown			2002 risk assessment
ECB 80	Request and review the physical and environmental documentation from the VDC. Include findings in the ECB SSP.	Closed	Concur			2002 risk assessment
ECB 82	Address the multiple findings in the personnel security portion of this assessment	Open	Unknown			2002 risk assessment

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 84	Incorporate the numerous logical access control findings into the ECB SSP	Open	Concur			2002 risk assessment
ECB 87	Obtain and review contingency plan and disaster recovery plan maintained by the VDC. ECB should ensure its business process will be restored at the VDC if a contingency or disaster occurs.	Open	Unknown			2002 risk assessment
ECB 1	There is no physical mailing address provided for Ms. Kay Jacks. In a future update please include the physical address.	Open	Concur			C&A Precert
ECB 2	Under 1.1, the MA is claimed to no be a system of record, yet evidence contained within the SSP and attachments suggests this is contradictory as names, SSN, dates of birth are parts of information processed by eCB. Please correct this as necessary here once the corrections in the other areas of the SSP are completed	Open	Nonconcur			C&A Precert

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 3	In 1.5, in the last paragraph it is stated that 4000 schools have access to this web site system; however, the true number of users is not disclosed here or under the users section of the SSP.Please either be more specific as to the number of users here and elsewhere it is appropriate, or remove this paragraph completely as it has no purpose in this section.	Open	Concur			C&A Precert
ECB 4	This section fails to identify the person(s) responsible for security administration of the eCB site/system and whom they report to. Please add more detail on who these people are, or explain who is designated with these responsibilities within the	Open	Nonconcur			C&A Precert
ECB 5	Section 1.6 does state that eCB is operational, it does not describe the appropriate system life cycle phase it is in, and what security phase the system is currently in.	Open	Nonconcur			C&A Precert

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 6	This section (1.7) does not adequately describe what a FISAP is, and what type of data is entered into a FISAP, and is subsequently processed via eCB. It does not adequately describe the type of information regarding individual uses at the school level that is retained by eCB. This section fails to describe the interconnection relationships in this general description and how eCB relates to them.	Open	Concur			C&A Precert
ECB 7	The SSP (1.8) fails to adequately discuss and identify the different types of users, their profiles, who authorizes their access etc. There is also no information on re-validation of users, the process used, and how often.	Open	Nonconcur			C&A Precert
ECB 8	This section (1.9) provides no numbers of how many servers make up the eCB, their IP addresses, location within the VDC, how many interconnecting FSA systems there are with eCB and what their IP addresses are. NO software license information or where it can be found or who is responsible for that information.	Open	Nonconcur			C&A Precert

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 9	This section (1.10) claims FSA policy does not require MOU's between interconnecting FSA systems, which is in conflict with ED and Federal regulations, policy, and guidance by NIST. The MOU's referenced here are devoid of any specific information regarding areas of security responsibility, points of contact, the terms of the interconnections and grounds for voiding the agreements.	Open	Concur			C&A Precert
ECB 10	There is no discussion (1.10) or description of Processing flow from system input to output t	Open	Concur			C&A Precert
ECB 11	The descriptions of interconnected systems or systems that the MA shares information with are very high level and vague. Previously undefined acronyms are used which makes the descriptions even harder to understand.	Open	Concur			C&A Precert
ECB 12	Re: Reference to SSPs for interconnected systems or systems that the MA shares information with, or short discussion of security concernsMany are made, but no other information or points of contact for their location are provided. No specific document names are provided either which would make it difficult to verify any information provided here.	Open	Unknown			C&A Precert

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 13	Re: Applicable Laws and Regulations (1.11)(Laws, regulations, and guidance documents, establishing requirements for the system)Many references are outdated and more recent IT security laws like FISMA are missing as are new Department policy and guidance documents. Update the references pre the SSP	Open	Concur			C&A Precert
ECB 14	This section (1.10) has a major contradiction between paragraph 2 on pg 16, and paragraph 4. This section also contradicts information provided in the MOU's regarding the type and sensitivity of the data processed by eCBS.	Open	Unknown			C&A Precert
ECB 15	Re: Confidentiality (1.1.2.1)(Justification for the confidentiality rating of the system)Not clearly explained and contradicts information provided in the MOU's and elsewhere in the SSP regarding the confidentiality of data processed by eCBS.	Open	Concur			C&A Precert
ECB 16	Confidentiality is identified as either High, Medium, or Low (1.1.2.1)	Open	Nonconcur			C&A Precert

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 17	(1.1.2.3) It is not made clear what the impact would be if eCB were not available to its users for any specified period of time. The risk assessment information is two years old and cannot be considered as viable accurate information. This also calls into question the viability of the current situation should eCB not be available and its impact to the processing of school loan and grant data.	Open	Concur			C&A Precert
ECB 18	Availability is not identified as either High, Medium, or Low (1.1.2.3)	Open	Nonconcur			C&A Precert
ECB 19	Re: Criticality (Description of the criticality of the system) There is no information provided in this section (1.1.2.4) that discloses the results of the CIP questionnaire results, or where in the FSA business process eCBS places with regards to mission criticality for FSA as a business function.	Open	Concur			C&A Precert
ECB 20	The criticality of the system is NOT identified as either Mission Critical, Mission Important, or Mission Supportive)	Open	Concur			C&A Precert

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 21	The risk assessment referenced is over a year old and was directed towards a mainframe system, not eCBS.	Open	Noncur			C&A Precert
ECB 22	No discussion of the methodology on identifying threats is discussed here. The table of findings and recommendations does not include corrective action milestones and dates of completion, and whether these findings have been fixed. There is no reference as to where this full risk assessment document can be found and who the point of contact is to obtain it.	Open	Unknown			C&A Precert
ECB 23	This section (2.2, Review of Security Controls) is not properly addressed. No corrective action plan is provided, nor is the location of where the record can be obtained.	Open	Concur			C&A Precert
ECB 24	The findings provided in section 2.1 are from an assessment done in May 2002, yet another risk assessment cited in 2.2 is dated in November 2001. Please resolve which risk assessment applies, provide the corrective action plan and the dates corrective action were	Open	Concur			C&A Precert

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 25	This section (2.3) does not address the users at the schools level. Please provide information on how school level users obtain and acknowledge rules of behavior for accessing this system. In addition, Figure 1, it is not apparent where the form starts and ends in relation to the text of the SSP. Please break out an actual formatted copy of the rules that the user signs and us it as an actual example.	Open	Concur			C&A Precert
ECB 26	School users are not addressed (2.3)	Open	Concur			C&A Precert
ECB 27	The Rules of Behavior do not include appropriate limits on interconnections to other systems (2.3)	Open	Concur			C&A Precert
ECB 28	The rules of behavior for this MA are included as an appendix and referenced within this section, or are included directly within this section					C&A Precert

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 29	Re: System Life Cycle (2.4)The first paragraph on page 34 and the fourth paragraph conflict regarding what phase of the life cycle the eCBS system is in. Please correct this. The second paragraph is not clearly worded and the third paragraph cites past events as upcoming milestones. Please	Open	Nonconcur			C&A Precert
ECB 30	The lifecycle phase of the MA is not documented	Open	Nonconcur			C&A Precert
ECB 31	It is not stated in which phase of the lifecycle phase the system is currently in	Open	Concur			C&A Precert
ECB 32	There is no description of how security is handled within the documented MA lifecycle and how it is in accordance with the Department of Education Information Technology Security Systems Development Lifecycle	Open	Unknown			C&A Precert

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 33	Not stated whether the MA has or has not been authorized to operate	Open	Concur			C&A Precert
ECB 34	Date of authorization or date of authorization request not provided	Open	Concur			C&A Precert
ECB 35	Name of management official authorizing system to operate or name of management official requesting approval to operate is not provided	Open	Concur			C&A Precert
ECB 36	Personnel security section (3.1) cites old Department policy documents and needs to be updated. The section does not address access rights and how they are figured into security level determinations.	Open	Concur			C&A Precert
ECB 37	Re: Background Screening(Description of how security clearances are processed for system users)The wording implies all users, including school level users	Open	Unknown			C&A Precert

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 38	Re: Establishing User Access(Description of how user accounts are established)School level users are not addressed sufficiently	Open	Unknown			C&A Precert
ECB 39	Does not address how separation of duties will be achieved	Open	Nonconcur			C&A Precert
ECB 40	Does not address how school user accounts will be terminated	Open	Nonconcur			C&A Precert
ECB 41	Does not describe the location of where the system hardware and software are housed	Open	Nonconcur			C&A Precert
ECB 42	The date of the document suggests that a contingency planning test has been conducted since the last documented test in July 2002	Open	Concur			C&A Precert

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 43	The reference to the contingency plan shows version 00 dated 7/2002. Please correct this.	Open	Concur			C&A Precert
ECB 44	There is no description of the procedures for regular system and data backups of the system that are in place	Open	Concur			C&A Precert
ECB 45	There is no description of the type of information that is backed up and frequency of backups	Open	Concur			C&A Precert
ECB 46	The location of the backups is not defined	Open	Concur			C&A Precert
ECB 47	No description of Physical/environmental controls at off-site storage facility	Open	Concur			C&A Precert

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 48	No description of the continuity of support requirements for the system	Open	Concur			C&A Precert
ECB 49	software maintenance controls for the system are not fully described	Open	Concur			C&A Precert
ECB 50	Software copyright policy is not described	Open	Nonconcur			C&A Precert
ECB 51	Configuration management plan is not referenced	Open	Unknown			C&A Precert
ECB 52	Data integrity and validation controls implemented for the system are not described	Open	Unknown			C&A Precert

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 53	virus detection and eradication policies and procedures for the system are not described	Open	Unknown			C&A Precert
ECB 54	system documentation, including security documentation, maintained for the system, is not listed	Open	Unknown			C&A Precert
ECB 55	security awareness and training is not discussed	Open	Unknown			C&A Precert
ECB 56	Incident response handling for the application is not described, including application incident handling as well as steps taken by the GSS	Open	Unknown			C&A Precert
ECB 57	Authentication controls are not discussed	Open	Unknown			C&A Precert

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 58	Method of user authentication (User ID and password, token, etc.) is not discussed	Open	Unknown			C&A Precert
ECB 59	No description of how the access control mechanism supports individual accountability	Open	Unknown			C&A Precert
ECB 60	system specific password controls are not described	Open	Nonconcur			C&A Precert
ECB 61	Number of invalid access attempts allowed is not specified	Open	Nonconcur			C&A Precert
ECB 62	Not specified whether initial/default passwords must be changed	Open	Nonconcur			C&A Precert

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 63	Allowable password character set not defined	Open	Nonconcur			C&A Precert
ECB 64	Allowable password character length not defined	Open	Nonconcur			C&A Precert
ECB 65	Password aging not defined	Open	Nonconcur			C&A Precert
ECB 66	Password enforcement not defined	Open	Nonconcur			C&A Precert
ECB 67	No definition of number of generations of expired passwords disallowed	Open	Nonconcur			C&A Precert

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 68	No procedures for handling lost and compromised passwords	Open	Nonconcur			C&A Precert
ECB 69	Required frequency of password changes not defined	Open	Nonconcur			C&A Precert
ECB 70	Enforcement of periodic password changes not discussed	Open	Nonconcur			C&A Precert
ECB 71	Logical Access Controls not described	Open	Nonconcur			C&A Precert
ECB 72	access privileges are not described	Open	Nonconcur			C&A Precert

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ECB 73	system specific session controls are not described	Open	Nonconcur			C&A Precert
ECB 74	process for re-certifying users is not described	Open	Nonconcur			C&A Precert
ERMS 9	Ed and service provider vulnerability to bomb threats	Closed	Concur			2002 risk assessment
ERMS 10	Physical access to Richmond and St. Paul facilities not adequately tested	Open	Concur			2002 risk assessment
ERMS 11	Telecommunications failure could disrupt system availability	Closed	Concur			2002 risk assessment

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ERMS 12	Inherent Internet Explorer vulnerabilities allow hacking of DoS attacks to system	Closed	Concur			2002 risk assessment
ERMS 13	Inherent MS internet information server vulnerabilities allow spoofing or masquerading attacks on system	Closed	Concur			2002 risk assessment
ERMS 14	Inherent MS NT vulnerabilities allow hacking or DoS attacks to system	Closed	Concur			2002 risk assessment
ERMS 15	Inherent user access and authentication vulnerabilities could create Privacy Act violations	Closed	Concur			2002 risk assessment
ERMS 1	The configuration management plan does not contain current version numbers of system software	Unknown	Unknown	11/17/2003		C&A

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ERMS 2	The configuration management plan does not demonstrate that system software has been properly licensed	Unknown	Unknown	11/17/2003		C&A
ERMS 3	Audit trails are not recorded, reviewed, or retained for 1 year, as required by FSA policy	Unknown	Unknown	11/17/2003		C&A
ERMS 4	Warning banners are not displayed, as required, on every login screen	Unknown	Unknown	11/17/2003		C&A
ERMS 5	Passwords do not meet complexity criterion	Unknown	Unknown	11/17/2003		C&A
ERMS 6	There is no separation of duties	Unknown	Unknown	11/17/2003		C&A

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
ERMS 7	There is no designated system owner	Unknown	Unknown	11/17/2003		C&A
ERMS 8	There are no documented procedures describing creation of emergency passwords	Unknown	Unknown	11/17/2003		C&A
ezAudit 1	The dept. has not fully implemented a risk-based, comprehensive agencywide security program that ensures the adequate application of security controls	Closed	Concur			2002 POAM
FMS 1	Plain text files transmitted--FMS III data files are not being encrypted during transmission. The deisgn and implementation of an encryption solution is required (note: in the corrective action plan POAM risk assessment report, this is number FSA-FMS-20)	Closed	Concur			2002 risk assessment
FMS 2	First-use passwords present an opportunity for unauthorized access (note: in the corrective action plan POAM risk assessment report, this is number FSA-FMS-19)	Unknown	Unknown			2002 risk assessment

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
FMS 3	Failure to provide a warning to visitors upon access to FMS may hinder the agency's ability to prosecute those engaged in malicious activity (note: in the corrective action plan POAM risk assessment report, this is number FSA-FMS-22)	Unknown	Concur			2002 risk assessment
FMS 4	Password vulnerability: Dept. of Ed. Password procedure is not being consistently applied (note: in the corrective action plan POAM risk assessment report, this is FSA-FMS-24)	Unknown	Concur			2002 risk assessment
FMS 5	FMS is vulnerable to sniffers (note: in the corrective action plan POAM risk assessment report, this is FSA-FMS-25)	Unknown	Unknown			2002 risk assessment
FMS 6	Sharing of Disparate Applications on the Same Server - The compromise of any one application on the servers shared by FMS could lead to any one of a number situations including the collapse of FMS' communications channels or a denial of service to certain applications for potentially prolonged periods. Such failure could result in compromise of critical applications or its data. (paragraph 2.2.2.3.1) (NOTE: In the Corrective Action Plan POA&M Risk Assessment Report, this is Number FSA-FMS-26 .)	Unknown	Unknown			2002 risk assessment

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
FMS 7	Change managers were unable to provide evidence that a change (selected for testing) had properly passed through the FMS change control procedures	Unknown	Unknown	11/1/2003		IGIC-03
FMS 8	A revalidation of user access rights to FMS had not been performed during the current audit period	Unknown	Unknown	11/1/2003		IGIC-03
FMS 9	There is no evidence that access-control security logs are being reviewed by security adminstrators	Unknown	Unknown	11/1/2003		IGIC-03
IFAP 1	Rules of behavior have not been established	Closed	Concur			2002 risk assessment
IFAP 2	The system does not contain a warning banner at systemn login	Closed	Concur			2002 risk assessment

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
IFAP 3	Security awareness training is not provided for IFAP users	Closed	Concur			2002 risk assessment
IFAP 4	Users are not periodically recertified	Closed	Concur			2002 risk assessment
IFAP 5	Unlimited concurrent logins are allowed	Open	Nonconcur			2002 risk assessment
IFAP 6	Inactive user sessions are not terminated after a period of inactivity	Closed	Concur			2002 risk assessment
IFAP 7	There are no formalized terminatino/transfer procedures established for IFAP	Closed	Concur			2002 risk assessment

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
IFAP 8	Remote registry access is not restricted to administrators	Closed	Concur			2002 risk assessment
NSLDS 1	The configuration management plan does not contain current version numbers of system software	Unknown	Unknown	11/17/2003		C&A
NSLDS 2	The configuration management plan does not demonstrate that system software has been properly licensed	Unknown	Unknown	11/17/2003		C&A
NSLDS 3	The system security plan neither identifies nor describes the software configurations	Unknown	Unknown	11/17/2003		C&A
NSLDS 4	The continuity of support plan has not been tested annually as required by Ed. policy	Closed	Unknown	11/17/2003		C&A

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
NSLDS 5	The security plan does not clearly define the job responsibilities of NSLDS security adminstrators	Unknown	Unknown	11/1/2003		IGIC-03
NSLDS 6	There is no documented procedure and/or requirement to monitor NSLDS' compliance with FSA security regulations and guidelines.	Unknown	Unknown	11/1/2003		IGIC-03
NSLDS 7	The password guidelines documented in the security plan do not fully comply with those required by FSA policy and the Department of Education Handbook for Information Technology Security Policy.	Unknown	Unknown	11/1/2003		IGIC-03
NSLDS 8	The current process to remove terminated employee accounts from the NSLDS appplication is not operating effectively	Unknown	Unknown	11/1/2003		IGIC-03
OCTS 3	User terminatioin and transfer procedures have not been documented	Closed	Concur			2002 risk assessment

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
OCTS 4	A warning banner is not displayed before user login	Closed	Concur			2002 risk assessment
OCTS 5	Users are not aware of responsibilities regarding implementation of the contingency plan.	Open	Concur			2002 risk assessment
OCTS 1	The configuration management plan does not demonstrate that software in the system has been properly licensed.	Unknown	Unknown	11/7/2003		C&A
OCTS 2	No documented procedures regarding actions to be taken when unsuccessful logon attempts are exceeded	Unknown	Unknown	11/7/2003		C&A
PEPS 2	PEPS does not have a method of enforcing minimum password standards	Closed	Concur			2002 risk assessment

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
PEPS 4	PEPS does not have a logon banner warning unauthorized users that they have accessed a US government system and can be punished	Closed	Concur			2002 risk assessment
PEPS 5	Code and data backups are kept on site	Closed	Concur			2002 risk assessment
PEPS 6	The current PEPS system configuration is not fully documented or distributed among key personnel	Closed	Concur			2002 risk assessment
PEPS 1	The system security plan does not clearly define the accreditation boundary	Unknown	Unknown	11/18/2003		C&A
PEPS 3	There was no evidence of MOUs or TPAs, or that the interfaces had been addressed in the SSP	Open	Unknown			EDS vulnerability assessment A-130

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
SAIG 3	SSP does not provide proper password guidance regarding password age	Closed	Concur			2002 risk assessment
SAIG 4	Users are not periodically recertified	Open	Unknown			2002 risk assessment
SAIG 1	The configuration management plan does not demonstrate that system software has been properly licensed	Unknown	Unknown	11/17/2003		C&A
SAIG 2	Group users IDs are not limited to an “as necessary” basis	Unknown	Unknown	11/17/2003		C&A
SAIG 5	There is no formal confirmation of the new employees acknowledging an understanding of the security awareness guidelines	Unknown	Unknown	11/1/2003		IGIC-03

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
SAIG 6	There are no yearly security awareness reeducation rebriefs taking place as discussed in the SAIG and VDC security manual	Unknown	Unknown	11/1/2003		IGIC-03
SAIG 7	There are no formal policies and procedures for conducting periodic reviews of user access privileges for SAIG employees, as well for developers working at NCS Pearson (who have access to SAIG)	Unknown	Unknown	11/1/2003		IGIC-03
SAIG 8	There are no formal policies or procedures for conducting periodic reviews of user access privileges for the Mainframe, Unix, and Windows NT environments	Unknown	Unknown	11/1/2003		IGIC-03
SAOTW 1	The configuration management plan does not document that the software for the system has been properly licensed	Unknown	Unknown	10/23/2003		C&A
VDC 59	Strengthen intrusion detection system--adjust monitoring activities	Unknown	Concur			2002 IG GISRA

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
VDC 60	Address SNMP vulnerabilities--investigate community of interest adjustments	Unknown	Unknown			2002 IG GISRA
VDC 56	Dial-in access is not being audited	Closed	Unknown			2002 risk assessment
VDC 57	Security awareness training is not being performed	Unknown	Unknown			2002 risk assessment
VDC 52	The configuration management plan does not state that system releases must be tested and debugged in a dedicated, controlled environment	Unknown	Unknown	9/11/2003		C&A
VDC 53	The configuration management plan does not require that software patches are tested	Unknown	Unknown	9/11/2003		C&A

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
VDC 54	Telnet, which has many known security issues, is currently deployed in the VDC environment	Unknown	Unknown	9/11/2003		C&A
VDC 55	Security awareness training and education does not meet federal guidelines	Unknown	Unknown	9/11/2003		C&A
VDC 49	Disaster recovery exercises do not adequately test contingency plan viability and recovery team preparedness.	Unknown	Unknown			IG
VDC 50	Planning activities do not ensure that IT contingency plans are current and complete	Unknown	Unknown			IG
VDC 51	The Department has not established an effective coordination of IT contingency planning issues associated with complex system interfaces and interdependencies	Unknown	Unknown			IG

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
VDC 58	Strengthen intrusion detection system--strengthen response to internal activity	Unknown	Unknown			IG

All FSA Findings—Open, Closed, and Unknown

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
VDC 1	· The VDC and EDNet system security plans identified broad policies for technical security controls but the specific procedures that are needed to enforce the policies have not been defined within the system security plans. For instance, the security plan specifies the minimum password requirement for all users but not identify the procedures of how this policy will be enforced on all platforms. We also noted that the system security plans did not address the specific responsibilities for system administrators, network administrators and database administrators in the following areas: 1) enforcing complex password policies for all accounts; 2) removing all default user accounts and passwords; 3) maintaining all host servers and network devices with the required system security patches and system updates to eliminate common vulnerabilities and exposures; 4) periodically reviewing the security settings of host servers, databases, and network devices for security weaknesses; 5) administration of firewalls, databases, and other network devices; 6) establishing formal logging procedures and periodic review of audit logs for system administering network administrators and database administrators; and 7) system monitoring and incident response procedures for administrators.	Open	Concur	11/7/2003		IG-Audit

All FSA Findings—Open, Closed, and Unknown

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
VDC 2	We noted that an IDS system, independent of the network firewall, had not been implemented to identify potential network intrusions and to protect mission critical servers supporting DLSS. In addition, we noted that administrators at the VDC have not fully deployed network based IDS systems to protect all network segments. NIST 800-18 states the importance of having intrusion detection tools in place for effective data integrity controls and an effective incident response capability.	Open	Concur	11/7/2003		IG-Audit
VDC 3	Based on our review of the Department's internal "Risk Assessment Reports," program officialsrepresent that all mission critical systems have controls to ensure that all employees receivemandatory periodic computer security awareness and training. During our review of thePrincipal Office's security awareness and specialized training programs, we noted thatcontractors supporting Department mission critical systems at the RCC, VDC, and on EDNet hadnot received the required computer security awareness training and specialized computer securitytraining sponsored by the Department.	Open	Concur	11/7/2003		IG-Audit

All FSA Findings—Open, Closed, and Unknown

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
VDC 4	· During our testing of password controls at the VDC, we identified: 1) passwords for 45 NTuser accounts; and 2) passwords for 169 UNIX user accounts, including three administratoraccounts. For the passwords identified, we noted that 15 user accounts had simple passwordsthat included identical user account names and password combination or the word“password.”	Open	Concur	11/7/2003		IG-Audit
VDC 5	We identified many servers (VDC = 98 and EDNet = 11) providing telnet services used for remote administration capabilities. Telnet service does not encrypt username, passwords, or transmitted data and is therefore vulnerable to sniffer attacks	Open	Concur			IG-Audit
VDC 6	We identified many servers (RCC = 12, VDC = 8, and EDNet = 11) using trust-based services such as “Rlogin” and “Rshell” which are vulnerableto well-known IP spoofing attacks that allow an attacker to execute commands from a trusted host. In addition, “Rlogin” passwords are transmitted in clear text and are therefore vulnerable to an attacker gaining passwords through sniffing activities.	Open	Concur			IG-Audit

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
VDC 7	We discovered many servers at the VDC using a version of SSH server that allows an attacker to use brute force techniques to determine usernames and passwords without this activity being logged by a server	Open	Unknown			IG-Audit
VDC 8	We identified many servers (VDC = 27 and EDNet = 4) using a version of Apache web server, that is susceptible to buffer overflow attacks, which could allow an attacker to view the Apache password file.	Open	Unknown			IG-Audit
VDC 9	We identified many servers (RCC = 4 and VDC = 14) that are using a version of Sendmail, which is susceptible to several well-known vulnerabilities, such as providing an attacker with an opportunity to corrupt certain databases or Denial of Service attacks.	Open	Unknown			IG-Audit
VDC 10	We identified several servers (VDC = 1 and EDNet = 2) that have configured the Network File System (NFS) mount to provide access to all users. The NFS mount should be restricted to authorize users since an attacker could possibly mount the share and read files on the	Open	Unknown			IG-Audit

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
VDC 11	On most Oracle databases tested (VDC = 5 and EDNet = 2), we noted that auditing for system events is not enabled and the Audit Trail Table is not defined to its own system table space to avoid possible storage capacity limitations. Oracle auditing can be set to log audit data to the database or operating system	Open	Concur			IG-Audit
VDC 12	On most Oracle databases tested (VDC = 7, RCC = 1, and EDNet = 3), we noted that the “DBLINK_ENCRYPT_LOGIN” or the "ORA_ENCRYPT_LOGIN" parameter settings is not configured to encrypt stored passwords or encrypt users passwords when users connect to the database. Unencrypted passwords are vulnerable to an attacker gaining passwords through sniffing activities.	Open	Concur	11/10/2003		IG-Audit
VDC 13	On most Oracle databases tested (VDC = 7 and EDNet = 4), we noted that the PASSWORD REUSE TIME parameter was not configured to limit the number of days that an application password can be reused.Consequently, no controls have been implemented to limit the use of recycled passwords.	Open	Concur	11/10/2003		IG-Audit

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
VDC 14	We noted that the routers at the RCC and the VDC have not adequately defined an ACL to limit the number of Telnet (Virtual TypeTerminal (VTY) ports) connections and corresponding IP addresses that are able to log onto the router. We noted that certain Telnet ACLs permit access from an entire class of IP addresses.	Open	Concur	11/10/2003		IG-Audit
VDC 15	We noted that two routers at the VDC have not defined the “enable secret” parameter which uses a strong, one-way encryption algorithm to protect system passwords. This parameter setting should be used in place of the “enable password” command, which does not adequately protect system passwords.	Open	Concur	11/10/2003		IG-Audit
VDC 16	We noted that routers at RCC and the VDC have not defined IOS – Exec Timeout parameter on all console and auxiliary interfaces. This parameter forces idle router logins to be disconnected in five minutes and therefore minimizes the risk of unauthorized use of abandoned console and auxiliary interface sessions.	Open	Concur	11/10/2003		IG-Audit
VDC 17	We noted that the routers at the RCC and the VDC have not enabled this service to terminate connections if the host on the other end of an idle connection has been lost.	Open	Concur	11/10/2003		IG-Audit

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
VDC 18	We noted that the IOS – Logging Buffered parameter had not been implemented on most routers to ensure that routers will store logged messages in a memory buffer and to assist in resolving network connectivity problems.	Open	Concur	11/10/2003		IG-Audit
VDC 19	We noted that the routers at the RCC, VDC, and one router on EDNet have not defined the IOS – NTP Server/Source parameter that isrequired for communication and time synchronization with other NTP servers.	Open	Unknown			IG-Audit
VDC 20	We noted that the routers at the RCC and VDC have not defined this parameter to ensure that only telnet connections are allowed for remotely accessing routers and will ensure that other unsecured protocols (e.g. rlogin, WWW) can	Open	Concur	11/10/2003		IG-Audit
VDC 21	We noted that one router at the VDC has not defined IOS – No Finger Service parameter to disable the finger service in accordance with vendor recommended settings.	Open	Unknown			IG-Audit
VDC 22	We noted that most routers at the RCC and the VDC have not defined this parameter to disable the Bootp service in accordance with vendor recommended settings.	Open	Unknown			IG-Audit

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
VDC 23	We noted that the routers at the VDC had not enabled this service so that the Cisco routers can send their log messages to a Unix-style syslog server.	Open	Concur	11/10/2003		IG-Audit
VDC 24	We noted that the routers at the RCC and the VDC had not enabled this service to ensure that logging messages are timestamped.	Open	Concur	11/10/2003		IG-Audit
VDC 25	We noted that domain controllers at the RCC, VDC, and EDNet were not configured to disable LANMAN user authentication over the network. The LAN Manager authentication encrypts only the first seven characters of a password, making passwords vulnerable to sniffing and passwordcracking tools such as "LOphtcrack."	Open	Concur	11/10/2003		IG-Audit
VDC 26	We noted that on most servers tested (RCC = 7 and VDC = 1), the Power Users, Administrators, and Server Operators had permission to perform this function.	Open	Concur	11/10/2003		IG-Audit

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
VDC 27	We noted that on most servers tested (RCC = 10 and VDC = 8), Administrators had permission to perform these functions.	Open	Concur	11/10/2003		IG-Audit
VDC 28	We identified several servers (RCC = 5 and VDC = 2) that were not configured to collect successful and unsuccessful attempts to access protected files and objects.	Open	Concur	11/10/2003		IG-Audit
VDC 29	We discovered that on most servers tested (RCC = 6 and VDC = 7), this setting was not configured to prevent unauthorized users from bypassing Windows NT authentication processes and gaining administrator privileges.	Open	Concur			IG-Audit
VDC 30	We noted that on most servers tested (RCC = 10, VDC = 2, and EDNet = 10), this setting was not configured to prevent displaying the last user's account name during subsequent logon sessions. Providing a user account name can assist an attacker in gaining unauthorized access to critical resources.	Open	Concur			IG-Audit

All FSA Findings—Open, Closed, and Unknown

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
VDC 31	We discovered that most servers (RCC = 2 and VDC = 10) had not configured this setting to allow Administrators to force users to log off when needed. This functionality may assist administrators in removing unauthorized users from system resources.	Open	Concur	11/10/2003		IG-Audit
VDC 32	We identified two HP-UX servers at the VDC where the number of system users exceeds the number of authorized users in accordance with the software license agreement.	Open	Unknown			IG-Audit
VDC 33	We noted that a number of servers (RCC = 2, VDC = 5, and EDNet = 4) contained files that were assigned permissions allowing any user to access certain files and directories, modify their contents, and execute various functions. We also identified world writeable configuration files in the /etc directory that provide for any process to have the ability to alter the configuration of the system seizing unauthorized resources or denying resources to authorized users. Excessive permissions may allow an unauthorized person to reconfigurecritical system files and compromise the integrity of the operating system.	Open	Unknown			IG-Audit

All FSA Findings—Open, Closed, and Unknown

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
VDC 34	We noted that a number of servers (RCC = 1, VDC = 10, EDNet = 1) were experiencing disk utilization rates greater than 90 percent and therefore may not have sufficient disk capacity to perform normal logging functions. Consequently, an attacker can force the log file to overflow and gain access to critical systems files without being detected by logging mechanisms.	Open	Concur			IG-Audit
VDC 35	We identified several servers (RCC = 3 and VDC = 2) containing hosts.equiv and rhosts files which indicates that trust relatio nships have beenestablished with other systems on the network. In addition, we noted that these files contain a root user account, which may allow an attacker to gain unauthenticated access to other trusted systems with administrator privileges.	Open	Concur			IG-Audit
VDC 36	We identified several servers (VDC = 3 and EDNet = 3) that contain duplicate user IDs that may allow a system user to masquerade unauthorized activity.	Open	Concur			IG-Audit

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
VDC 37	We identified two servers at the VDC that contain shadow files that do not include all user account passwords from the “passwd” file listing. User accounts and passwords not included in shadow files are vulnerable for exploitation since the passwords are seen by all accounts and can be downloaded	Open	Concur			IG-Audit
VDC 38	We noted that a number of system programs remain defined to the RACF Program Property Table, which allows those programs to bypass normal RACF authorization processes.* CPS 10 programs defined* PELL 11 programs defined* NSLDS 10 programs defined* FFEL 12 programs defined	Open	Concur	11/10/2003		IG-Audit
VDC 39	15 Web Servers contain CGI Vulnerabilities that may allow an attacker to view certain file directories of the web server.	Open	Concur	10/30/2003		IG-Memo
VDC 40	15 Web Servers contain CGI Vulnerabilities that may allow an attacker to view certain file directories of the web server.	Open	Concur	10/30/2003		IG-Memo

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
VDC 41	15 Web Servers contain CGI Vulnerabilities that may allow an attacker to view certain file directories of the web server.	Open	Concur	10/30/2003		IG-Memo
VDC 42	15 Web Servers contain CGI Vulnerabilities that may allow an attacker to view certain file directories of the web server.	Open	Concur	10/30/2003		IG-Memo
VDC 43	15 Web Servers contain CGI Vulnerabilities that may allow an attacker to view certain file directories of the web server.	Open	Concur	10/30/2003		IG-Memo
VDC 44	An Internet facing Web Server using an outdated version of Netscape Enterprise Web Server that is susceptible to brute force attacks, buffer overflow attacks, and unauthorized file disclosure vulnerabilities.	Open	Concur	11/7/2003		IG-Memo
VDC 45	19 Windows NT Servers that utilize an outdated version of Compaq Web Management Server (CWMS),….	Open	Concur	10/30/2003		IG-Memo

System Name	Finding	Status	Concur/ Nonconcur	Date Reported	Date Closed	Sources
VDC 46	19 Windows NT Servers that utilize an outdated version of Compaq Web Management Server (CWMS),….	Open	Concur	10/30/2003		IG-Memo
VDC 47	Seven databases contain accounts with default usernames and passwords or accounts with identical username and passwords.	Open	Concur	10/30/2003		IG-Memo
VDC 48	22 Servers utilize Simple Network Management Protocol (SNMP) with the default passwords.	Open	Concur	10/30/2003		IG-Memo